CTF 101

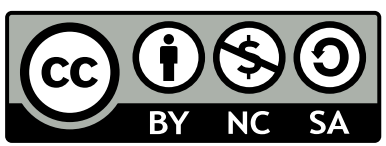
Ricardo J. Rodríguez

rjrodriguez@unizar.es ※ @RicardoJRdez ※ www.ricardojrodriguez.es

Universidad Zaragoza

Dpto. de Informática e Ingeniería de sistemas
Universidad de Zaragoza

17 de septiembre de 2019



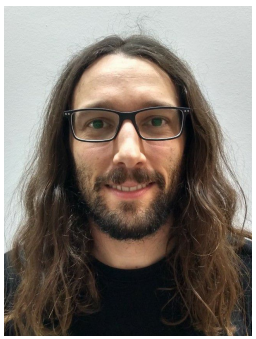
$whoami

- **Profesor en Universidad de Zaragoza**
- Líneas de Investigación:
  - Análisis de rendimiento/dependability/seguridad de sistemas
  - Análisis forense de programas binarios
  - Seguridad RFID/NFC
- Ponente y profesor técnico en conferencias profesionales de seguridad informática (NcN, HackLU, RootedCON, STIC CCN-CERT, HIP, MalCON, HITB...)
- Participante y **diseñador de pruebas** en CTFs ☺

Universidad Zaragoza
1542

$whoami

- **Profesor en Universidad de Zaragoza**
- Líneas de Investigación:
  - Análisis de rendimiento/dependability/seguridad de sistemas
  - Análisis forense de programas binarios
  - Seguridad RFID/NFC
- Ponente y profesor técnico en conferencias profesionales de seguridad informática (NcN, HackLU, RootedCON, STIC CCN-CERT, HIP, MalCON, HITB...)
- Participante y **diseñador de pruebas** en CTFs ☺
- Equipo de investigación: ***hacemos cosas chulas!***



Miguel Martín-Pérez
Estudiante PhD.

Daniel Uroz
Investigador

- Análisis forense
- Malware
- Exploiting vulns
- Reversing
- Red Tor

Universidad Zaragoza

¿Qué es un evento CTF?

¿Querías decir WTF?

- No! ◡̈

Universidad Zaragoza

¿Qué es un evento CTF?

¿Querías decir WTF?

- No! ◡̈

Universidad Zaragoza

¿Qué es un evento CTF?

- **Competición relacionada con la seguridad de la información**
- Los participantes se enfrentan a **diferentes retos, con el objetivo de conseguir una "flag"** para sumar puntos
  - Las *flags* suelen tener cadenas reconocibles, como `flag{5R0ck_m4t3!$}`
- **El equipo con más puntos es el que gana**

Universidad Zaragoza
1542

¿Qué es un evento CTF?

- Organizadas por empresas del sector informático (**atracción de talento**) o como **eventos paralelos a conferencias** de seguridad (MalCon, NcN, DEF CON, BSides, etc.)
- **Tipos de celebración**:
  - Fase on-line
  - Fase on-line + fase presencial
  - Fase presencial

Universidad Zaragoza
1542

¿Qué es un evento CTF?

- Organizadas por empresas del sector informático (**atracción de talento**) o como **eventos paralelos a conferencias** de seguridad (MalCon, NcN, DEF CON, BSides, etc.)
- **Tipos de celebración**:
  - Fase on-line
  - Fase on-line + fase presencial
  - Fase presencial
- **Tipos de premios**:
  - Económicos (metálico, productos, contrato de trabajo)
  - Esponsorización (entrada conferencia + viaje, etc.)
  - **Kudos!** ♥

Universidad Zaragoza
1542

Tipos de CTF

- ***Jeopardy***
  - Diferentes categorías de retos
  - Con diferentes puntuaciones y dificultades

Universidad Zaragoza
1542

Tipos de CTF

- ***Jeopardy***
  - Diferentes categorías de retos
  - Con diferentes puntuaciones y dificultades
- ***Attack-defense***
  - Cada equipo defiende una red o sistema
  - Todos se atacan entre todos
  - Se puede robar las *flags* a los contrarios

Universidad Zaragoza
1542

Tipos de CTF

- ***Jeopardy***
  - Diferentes categorías de retos
  - Con diferentes puntuaciones y dificultades
- ***Attack-defense***
  - Cada equipo defiende una red o sistema
  - Todos se atacan entre todos
  - Se puede robar las *flags* a los contrarios
- **Mezcla de ambos**

Universidad Zaragoza
1542

Pruebas típicas en un CTF

- **Web**
  - Búsqueda de vulnerabilidades en aplicaciones web
  - Conocimientos en SQL injection, XSS, etc.
- **Forense**
  - Análisis de paquetes de red, volcados de memoria, etc.
- **Criptografía** / **esteganografía**
  - Descifrado de cadenas cifradas usando cifrados de substitución o similares
  - Detección de información oculta
- **Ingeniería inversa** (reversing)
  - Análisis estático y dinámico de binarios
- **Explotación**
  - Construir un exploit para una vulnerabilidad de una aplicación
  - Puede ser orientado a binarios o a Web
  - Normalmente se proporciona el código fuente, a diferencia del *reversing*
- **Redes**
  - Cosas relacionadas con redes
- **Miscelánea**
  - Otras cosas no listadas pero relacionadas con seguridad (e.g., programación segura)

Participando en un CTF
Habilidades

- ***Google-Fu***
  - Saber buscar en Google es importante (y no sólo para esto)
  - Búsqueda de pruebas similares en otros CTFs
- **Conocimientos de scripting** (Perl, Python, bash, etc.)
  - Útil para automatización de tareas y generación de exploits
- **Conocimientos de Linux**
  - Saber usar la consola es importante. Multitud de herramientas nativas: `cat`, `nc`, `strings`, `file`, `grep`, `vim`, `base64`, `binwalk`, `Exiftool`, `gdb`, y un largo etcétera
- **Conocimientos de pentesting**
  - Conocimiento de vulnerabilidades web más comunes (OWASP top 10)

Participando en un CTF

Habilidades

- **Conocimientos de ingeniería inversa** (*reversing*)
  - Hay que saber analizar un programa binario, tanto PE como ELF
  - Algunos CTFs ponen pruebas incluso con binarios de arquitecturas muertas o inventadas (máquinas virtuales)
  - Conocimientos de ensamblador y de arquitectura de computadores básicos
  - *¿Todavía no sabes programar en C?*
- **Conocimientos de explotación**
  - Reconocer vulnerabilidades en software comunes y cómo explotarlas
  - Normalmente requerirá habilidades de *reversing*
- **Conocimientos de red**
  - Conocimientos básicos de redes (protocolos, pila TCP/IP, etc.)
  - Uso de herramientas tipo Burp, Wireshark, etc.
- **Criptografía**
  - Reconocer algoritmos criptográficos
  - Conocer esquemas criptográficos con configuraciones incorrectas (e.g., uso de ECB, IVs constantes, etc.)

Universidad Zaragoza 1542

Participando en un CTF

Lista (no exhaustiva) de herramientas útiles

Créditos: `http://delimitry.blogspot.com/2014/10/useful-tools-for-ctf.html`

Participando en un CTF

Algunos consejos

Preparación para un CTF

- **Equipos multidisciplinares**
  - Difícil encontrar a una persona que sepa todo de todo
- **Planificar participación del grupo y roles**
  - Cada uno se compromete a jugar en un rango de horas
  - Equilibrar el equipo en todo momento (si es posible)
  - Definir dónde se va a jugar (suele ser bueno estar todos juntos)
  - **Importante**: definir un encargado de las pizzas, el café y la cerveza

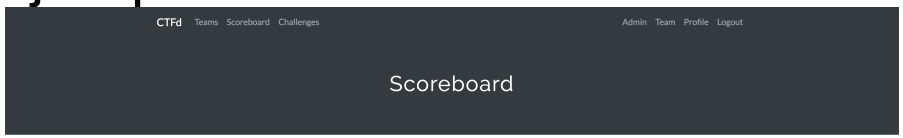
Trabajo individual

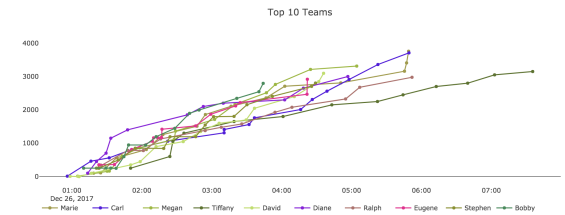
- **Repaso de otros CTFs** donde hayas participado
- **Repaso de pruebas anteriores** (en el mismo CTF)
- **Lectura de "write-ups"** (ejemplos de solución)
- *Use the Google, Luke!*

Universidad Zaragoza 1542

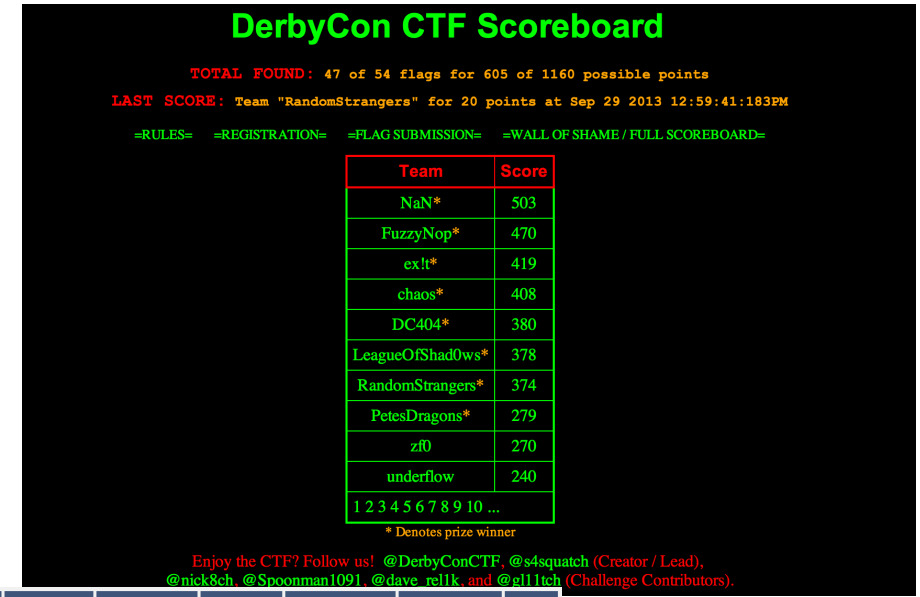
Participando en un CTF

Ejemplos de marcadores





Place	Team	Score
1	Marie	3759
2	Carl	3710
3	Megan	3313
4	Tiffany	3150
5	David	3097
6	Diane	3000



Rank	Team	ping4	ping6	1337f4x0r	catacombs	railway	smartgrid	bank	supermarket	trafman	Offense	Defense	Score
1		secure	secure	secure 0 captures 10 weight	good 3 captures 6 weight	secure 0 captures 10 weight	secure 0 captures 10 weight	good 1 captures 8 weight	secure 0 captures 10 weight	broken 0 captures 9 weight	9.76% (51791 points)	1.84% (4209 points)	5.80%
2		secure	secure	secure 0 captures 10 weight	broken 0 captures 10 weight	good 2 captures 7 weight	secure 0 captures 10 weight	good 1 captures 8 weight	good 1 captures 8 weight	secure 0 captures 10 weight	9.50% (50437 points)	1.97% (4490 points)	5.74%
3		secure	secure	secure 0 captures 10 weight	good 3 captures 6 weight	secure 0 captures 10 weight	secure 0 captures 10 weight	secure 0 captures 10 weight	secure 0 captures 10 weight	broken 0 captures 10 weight	8.86% (47006 points)	1.97% (4488 points)	5.41%
4		secure	secure	secure 0 captures 10 weight	broken 2 captures 7 weight	good 1 captures 8 weight	good 5 captures 4 weight	down 2 captures 7 weight	good 1 captures 8 weight	secure 0 captures 10 weight	6.65% (35292 points)	1.95% (4451 points)	4.30%
5		secure	secure	secure 0 captures 10 weight	broken 1 captures 7 weight	good 4 captures 5 weight	good 13 captures 2 weight	good 18 captures 1 weight	secure 0 captures 10 weight	broken 0 captures 9 weight	5.32% (28226 points)	1.98% (4523 points)	3.65%
6		secure	secure	secure 0 captures 10 weight	broken 1 captures 8 weight	secure 0 captures 10 weight	good 3 captures 6 weight	good 1 captures 8 weight	secure 0 captures 10 weight	broken 0 captures 9 weight	4.80% (25457 points)	1.99% (4531 points)	3.39%
7		secure	secure	secure 0 captures 10 weight	broken 2 captures 7 weight	secure 0 captures 10 weight	secure 0 captures 10 weight	good 1 captures 8 weight	secure 0 captures 10 weight	broken 0 captures 9 weight	3.98% (21144 points)	1.97% (4494 points)	2.98%
8		secure	secure	secure 0 captures 10 weight	broken 2 captures 7 weight	secure 0 captures 10 weight	broken 0 captures 10 weight	good 2 captures 7 weight	good 1 captures 8 weight	secure 0 captures 10 weight	3.74% (19830 points)	2.01% (4595 points)	2.88%

Créditos: Google Images

Participando en un CTF

Recursos de interés

- **Plataforma ATENEA del CCN-CERT**
  - https://www.ccn-cert.cni.es/soluciones-seguridad/atenea.html
- **CTFHacker** (http://ctfhacker.com/)
- **CTFtime** (https://ctftime.org/)
- **Root-Me** (https://www.root-me.org)
- **Wechall** (https://www.wechall.net/)
- **OverTheWire** (http://overthewire.org/wargames/)
- **Hack the Box** (https://www.hackthebox.eu/)
- **Google**
- **Otros enlaces de interés**:
  - http://fstm.kuis.edu.my/blog/what-is-ctf-capture-the-flag/
  - https://www.blogdelciso.com/2019/04/24/ctf-el-entrenamiento-necesario/

Universidad Zaragoza 1542

CTF 101

Ricardo J. Rodríguez

rjrodriguez@unizar.es ※ @RicardoJRdez ※ www.ricardojrodriguez.es

Universidad Zaragoza

Dpto. de Informática e Ingeniería de sistemas
Universidad de Zaragoza

17 de septiembre de 2019